CRYPTO A.M.

Our series on AI, Blockchain, Cryptoassets, DLT and Tokenisation

E: CryptoInsider@cityam.com @CityAm_Crypto

In association with CryptoCompare

PARTNER CONTENT

CITY A.M.'S CRYPTO INSIDER

JAMES BOWATER

Greetings from London where, with most people now back from annual leave, a plethora of fantastic projects are set to launch. Certainly my diary is literally back to back so there will be much to share with you in the coming weeks.

One person looking to sort out his near-term career plan is the Governor of the Bank of England, Mark Carney who, at the gathering of Central Bankers in Jackson Hole on 23rd August, suggested that a Libra like digital currency could usurp the US dollar as the defacto global reserve currency. Since his speech, others are joining the chorus not least of all the People's Bank of China who are set to release their own version of Libra perhaps as soon as the 70th Anniversary of the People's Republic of China which falls on 31st October. As reported in Forbes identified distributors of the digital currency will include the Industrial and Commercial Bank of China, the Bank of China, the Agricultural Bank of China; two of China's largest financial technology companies, Alibaba and Tencent; and Union Pay.

The market over the last week as been bouncing around but ended quite flat since last week's edition. Bitcoin (BTC) is down 3% from last week at US$9,915.23; Ethereum (ETH) is at US$173.28; Ripple (XRP) is at US$0.2576; Binance (BNB) is at US$22.54 and Cardano (ADA) is at US$0.04982. Overall Market Cap is at US$255.24bn (data source: www.CryptoCompare.com)

With the Amazon Rainforest being bulldozed and set fire to at an alarming rate everyone is jumping on this as a new political bandwagon. Yet this has been going on for decades with corporate agriculture being consistently blamed although leaked documents suggest something insidious in the form of wanton destruction of indigenous lands. Political leaders, NGO and other organisations citing the Amazon as the lungs of the world seem to favour banning such practices. That might help but it doesn't address the main issue which is simple economics - make it more commercially beneficial to undertake reforestation. Enter stage left AI, Blockchain and Cryptocurrency as a combination of technology as an administrative system for land registry, plant provenance and rewards. The UK's AI, Blockchain and Crypto ecosystem is more than capable of rising to the challenge!

MERJ Exchange and London based Globacap announced a partnership which will enable FCA licensed Globacap to distribute the upcoming MERJ token offering to UK and EU investors. I spoke with Jim Needham, head of digital asset strategy at MERJ, who explained "Part of the MERJ model is to build a global footprint of top tier partners. London is one of the leading cities for innovation in this space and Globacap have been at the forefront of that. They have shown a brilliant ability to execute and we are delighted to be working with them". The alliance brings together two companies intent on introducing international governance standards and safety nets to the world of digital assets through fully compliant end-to-end infrastructure.

FORMAL METHODS: MISSION-CRITICAL FOR SOFTWARE DEVELOPMENT?

Designed by Bowater Media

Phill Snelling,

WHAT ARE 'FORMAL METHODS'?

'Formal methods' is a way of writing program code using techniques that are well-founded in logic and mathematics, that allow you to reason 'formally' about your programs, ensuring that they are correct.

Of course, in order to determine whether computer code is correct, you have to have a very clear statement of what your program is actually meant to do. So the first step in using formal methods typically consists of writing a clear and unambiguous 'formal' specification that states the intended behaviour of the program.

From there, you can go on to prove properties of the specification itself, such as that there are no logical inconsistencies in it. Ideally, such proofs are produced using 'proof-assistants'. Those are computer programs that help writing proofs, and more importantly, that can check that the proofs are really correct.

Having proved that the specification is correct, the next step is to make sure the program behaves according to the specification.

THAT SOUNDS USEFUL. IS EVERYONE IN THE SOFTWARE INDUSTRY DOING THIS?

No. Unfortunately, using formal methods is pretty expensive, both in terms of money and time, so it is mainly used in areas where it's critical that you don't have bugs in your software. When you're programming rockets that send satellites into space, the smallest bug can be mission ending. When you're writing software for medical devices or aircraft, the smallest mistakes can kill people. So for those applications, investments in the correctness of your software are easily justified, and those are the main areas where formal methods have been heavily used.

When you are working on a product with less value at risk, current practice is that you use less rigour in development, ship something that mostly works, and then fix bugs as you or your users find them. It lets you go to market quickly, and since everyone is used to installing software updates - typically bug and security fixes, on a regular basis, there is little to no reputational damage.

Blockchains are typically not developed using formal methods, but they secure vast amounts of money, so I would argue that they should be.

IS THERE SOME KIND OF MIDDLE GROUND?

Yes, there is. You can use what are broadly termed 'lightweight formal methods', and that is what we are mostly focusing on at IOHK. We write specifications, but instead of writing them in a way that allows the computer to reason about them and prove things, we write them in a way that allows the computer to actually execute them, as a computer program. You can think of those executable specifications as a kind of carefully designed, high-level prototype, which glosses over the low-level details.

Ignoring the low-level details at this stage is actually very valuable because if tests fail, it's easier to identify why and make fixes. Also, it's much easier to develop the high-level design if you're not yet constrained by some concrete, detailed implementation choices. So you can solve all your hard problems early, on an abstract level, and fill in the details later.

At the end of the process, you have two programs: the 'high level' executable specification – lacking details and performance, but you're confident that it is correct; and the production implementation, that you want to give to your users. We systematically test these against each other.

SO YOU ARE DOING A LOT OF TESTING. DO YOU USE SPECIAL TECHNIQUES THERE?

Yes, we are using what is known as property based testing, another form of lightweight formal methods, much more powerful than writing test cases manually. The idea there is that instead of writing individual test cases, you write more general properties that you want to hold under all circumstances – things like "money does not appear or disappear from the system", "adding a transaction has the same effect in the executable specification and the production implementation", and similar statements. You then generate lots and lots of randomised test data, and check that those properties always hold.

WHAT IS YOUR VIEW ON FUTURE BROADER ADOPTION OF LIGHTWEIGHT FORMAL METHODS?

The major barrier to adoption is that it's often not easy to get buy in from customers. Part of that is just that it's not yet a recognised best practice, but another aspect boils down to making progress visible. In the software industry, people are used to an agile approach, where you deliver small parts of a software product in rapid succession. Using formal methods, solving the hard, fundamental, underlying problems on the spec level first, you are making a lot of progress, but without actually shipping something, so that progress is less visible. But our developers tell me that once you have that spec, filling in the details is a very pleasant and smooth exercise, and you end up with a better product that you can be confident in.

> My hope is that once we succeed, other companies will follow, and that ultimately the way that software is produced across the industry will improve

At IOHK, we understand the benefits of a formal methods approach and that it leads to better products and an overall reduction in costs for our clients. My hope is that once we succeed, other companies will follow, and that ultimately the way that software is produced across the industry will improve. You could argue that we are on a crusade!.

Charles Hoskinson, Founder & CEO of Input Output, in conversation with James Bowater. For more information visit https://iohk.io/

IMPORTANT INFORMATION: THE VIEWS AND OPINIONS PROVIDED BY CITY A.M.'S CRYPTO INSIDER AND IN THE CRYPTO A.M. SECTION SHOULD NOT BE TAKEN AS INVESTMENT OR FINANCIAL ADVICE. ALWAYS CONSULT WITH YOUR FINANCIAL ADVISOR.

CRYPTOCOMPARE MARKET VIEW

Bitcoin Drops Below $10,000, Facebook Hires Firm to Lobby for Libra

This week the price of bitcoin dropped below the $10,000 mark and hit a low of less than $9,400, at a time in which Facebook has hired a lobbying firm. The social media giant hired a lobbying firm that has experience with cryptocurrencies, and is believed to have been hired to help deal with lawmakers' concerns surrounding the company's proposed cryptocurrency - Libra. Facebook is yet to comment.

Telegram, a privacy-centric messaging app, is reportedly launching its cryptocurrency later this year. After raising over $1.7 billion through an initial coin offering, legal documents bind the firm to launch its cryptocurrency by 31st October of this year, as it was promised to investors that was the deadline.

Binance, a leading cryptocurrency exchange, has this week started offering lending services to its users, who can now earn up to 15% APR on their cryptocurrency holdings through its platform. Other exchanges, including Poloniex, Bitfinex, and OKEx also let users earn on their holdings.

Bakkt, a cryptocurrency venture by the owner of the New York Stock Exchange, has announced its users will be able to deposit funds to the Bakkt Warehouse on Sept. 6, ahead of its launch of physically-settled bitcoin futures contracts.

A man who claims to be the creator of Bitcoin, Craig Wright, was ordered by a Florida court to hand over 500,000 bitcoins - worth almost $5 billion - and intellectual property rights to the estate of his late business partner, David Kleiman. The court rejected Wright's testimony after finding he perjured himself for falsifying documents.

Finally, a study conducted by leading cryptocurrency exchange Coinbase has found that over half of the world's top universities now offer cryptocurrency classes to meet demand from students looking to know more about the nascent space.

CRYPTO A.M. INDUSTRY VOICES

Crypto and Blockchain could clean up malpractice within the fashion supply chain

The $800bn fashion industry is synonymous with waste, pollution, inhumane working conditions and slavery. 10% of all global emissions are caused by fashion. 40 million adults are in slavery worldwide and 264 million kids are not in school, many of these are as a direct result of fashion. Most of the 92 million tons of solid waste from fashion are buried in landfill or burnt, every year. Aside from the disastrous environmental practices associated to fashion - such as pouring toxic waste chemicals directly into rivers - 60% of clothes are made with plastic. This breaks down when worn and washed, into microfibers that get into water. In one test 73% of fish were found to have plastic in their stomachs. The fashion industry uses up excessive water at a time when some countries are running out.

WHAT DOES THIS HAVE TO DO WITH CRYPTO?

When it became more important to have fast, cheap fashion over anything else, production was outsourced to developing countries. Practices for recording environmental and employment processes tend to range from dubious to lacking. Supply chains are vastly complex, and there's also a large element of some not wanting to know. In one study, only 7% of brands had traced their raw materials. Blockchain allows data to be added to an immutable distributed ledger at every stage of a supply chain. In practice, this means that anyone in the entire supply chain can see exactly who entered what data, and whilst this data can continuously be added to, old entries can't be changed or deleted. If anyone adds any incorrect or implausible data, if any money goes unannounced for, or any purchases for environmentally damaging raw materials are made, anyone will be able to see who was responsible.

Using cryptocurrency in the global fashion supply chain would be the biggest change we could make. Cryptocurrency provides the full transparency of blockchain to every payment made. For large companies producing multiple ranges it is simply logistically not possible to oversee every transaction. One T-shirt range might be made in multiple different small factories, where local knowledge, culture and language is needed, so brands have to trust the many intermediaries between them and the factory. With crypto, every single token can be tracked and every transaction can be linked back to the last. Rules can be set about how payments can be made and where money can go, preventing unwanted transactions. This would give brands full control and visibility over exactly where every penny is spent, right back to seeing exactly what raw ingredients are bought, when those transactions were made, how much and who was being paid. Any discrepancies or lack of payments, such as to factory workers, would clearly stand out.

We have all the tech now in place for free, instant, traceable micro-transactions that would provide full accountability for every aspect of supply chain. The problem in implanting this is human. All parties in a supply chain would have to cooperate and would have to be fully transparent with each other, and change a lot of internal processes.

Using crypto and blockchain would allow brands to show exactly how much workers were paid, which factory clothes were made in, what the raw ingredients were, that no toxic dies were used, and possibly even how much water and environmental miles were used in their making. This information could go on every item of clothing made. Two otherwise similar items of clothing or brands could be compared for their environmental and ethical impact, allowing consumers to make accurate decisions on what they buy, and the impact of their purchases.

Erica Stanford is the founder of the Crypto Curry Club blockchain education events across the UK Email hello@cryptocurryclub. More info at ccc.events

Crypto A.M. shines its Spotlight on Lendingblock

Monolith Lending has become an explosive trend that is tearing through the crypto markets as of late.

With a number of players in the lending arena, who are all offering slightly different propositions, market participants have a variety of lending options to consider – margin lending, borrowing on leverage, secured lending, and the list goes on.

Crypto lending supply and borrowing demand have also been known not to falter amongst bouts of market volatility and bear markets. Actually, demand has only proven to increase. Despite this excitement, crypto lending is still very much in its early days and is representing what is still quite a fragmented market, lacking critical market infrastructure to help it mature. Amongst this backdrop, enter Lendingblock.

Lendingblock is the first exchange fully dedicated to pure crypto lending that aims to support the needs of the broader cryptocurrency market by providing a secure and liquid venue for lending and borrowing needs of institutional market participants. Lendingblock's regulated platform will act as a centralized global lending marketplace, and it is launching on September 3, 2019.

Upon launch, Lendingblock platform users will be able to borrow and lend BTC, ETH, PAX and USDT on a fully collateralized basis, for loan terms of 1, 7, 14 and 30 days, with a minimum trade size of $100,000 equivalent of a specified digital asset. Rates are set by the market supply and demand, providing a transparent view of prevailing market rates.

> Lendingblock plays an essential role in helping the institutional crypto lending market mature.

Steve Swain, CEO, Lendingblock

Clients include a mix of hedge funds, market makers, trading houses, OTC providers, crypto lending firms, and exchanges, and each have a need to either generate interest on an asset they are holding or would like to borrow in order to facilitate a specific strategy such as for shorting, arbitrage or working capital purposes. Lendingblock's market depth analysis charts, order book tools and risk-free yield curves provide clients with access to market data and price transparency across the global lending market.

Steve Swain, CEO, Lendingblock, said "We see the Lendingblock exchange as a key piece of market infrastructure that will provide efficiencies and support healthy markets in the crypto economy. We look forward to bringing the first institutional lending exchange to market and believe it will play an essential role in facilitating clients' trading strategies and also in helping the crypto market infrastructure to mature."

Darius Sit, Managing Partner at Singapore-based crypto trading firm, QCP Capital, said, "Having access to an institutional exchange where the lending supply and borrow demand is organized centrally and highly transparent in terms of being able to see the rates across different crypto assets and terms is something that the market most definitely should benefit from."

The Lendingblock platform can also be accessed via an API and will soon also be available through a variety of distribution partners, such as Caspian's order execution management platform. Lendingblock has 24-hour support over the phone and offers live chat to support clients throughout the process. Lendingblock, over the coming months, will also be expanding its capabilities to further meet client demand.

Find out more at https://lendingblock.com

TRUTH IN BLOCKCHAIN

Jon Walsh, Associate Partner Blockchain Rookies

Unlike how some people may suggest, Blockchain is not a silver bullet to solve the ails of any given industry. There are multiple challenges to make it work as intended – e.g. remove unneeded middlemen and create transparency on a supply chain.

Beyond the challenges of correct project governance and reaching consensus on standards, a major challenge is ensuring that all participants agree that the Blockchain truth, is the single source of truth.

Imagine a food supply chain on a Blockchain for organic eggs. Everyone from the farmer to the haulier to the warehouse all record the movement of the eggs through the supply chain. Now we, the egg buying public, can see by scanning a QR code on the side of the box the farm the eggs came from, the date they were laid and the whole supply chain through to the point where they wind up on the shelf of your favourite supermarket.

What is tracked in this scenario is effectively the cardboard egg box and not the eggs inside. This would be pretty easy for any farm or distributor to switch contents and make a significant profit by selling non-organic eggs masquerading as organic.

Alternatively, in the digital advertising supply chain, being able to track the flow of money from advertiser to publisher should be fairly simple as all payments would be recorded on the blockchain. However, it would still be easy for industry standard kick-backs to occur where there were no records on the blockchain to trace and audit.

A blockchain can provide a trusted source of truth which reduces fraud as well as time and costs of reconciliation of information between participants. Since not everything can (or even should) be put on the Blockchain, it's the truth – but it may not be the whole truth.

Get in touch with us info@blockchainrookies.com / Twitter @igetblockchain